August 2012

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

DEFENSE HORIZONS
National Defense University

Preparing the Pipeline: The U.S. Cyber Workforce for the Future

by David J. Kay, Terry J. Pudas, and Brett Young

About the Authors

David J. Kay is a Research Analyst in the Center for Technology and National Security Policy (CTNSP), Institute for National Strategic Studies, at the National Defense University. Terry J. Pudas is a Senior Research Fellow in CTNSP. Brett Young was a Research Assistant in CTNSP.

Key Points

- There is widespread agreement in the public and private sectors that U.S. educational institutions are unable to meet the growing demand for cyber workforce professionals.
- It is difficult to measure the true size and requirements for the cyber workforce due to the lack of commonly agreed upon cyber workforce job titles and duty descriptions.
- The Federal Government should develop additional methods for streamlining the hiring and contracting of essential cyber talent and emphasize the recruitment of cyber workforce professionals with demonstrated competency.
- Federal, state, and local governments must compete with the private sector, academia, and international actors to recruit and hire top cyber workforce professionals.
- Innovative solutions should be increasingly used to get students engaged in science, technology, engineering, mathematics, and cyber studies in order to develop skills in secondary and postsecondary students and to recruit them for government service later in life.

In 2008, the Comprehensive National Cybersecurity Initiative listed "expanded cyber education" as one of its key recommendations. In 2009, the Partnership for Public Service produced a report stating that the current pipeline of cybersecurity workers into the government was inadequate.[1] In the same year, Secretary of Defense Robert Gates stated that the military was "desperately short of people who have the capabilities [to operate in cyberspace]."[2] And in 2011, the Inspector General of the Federal Bureau of Investigation reported that 35 percent of the special agents investigating national security cyber-intrusion cases lacked necessary training and technical skills.[3] Nonetheless, the U.S. Government and private sector still seek to increase their online operations and dependency in spite of these shortcomings. An expert at the Atlantic Council of the United States sums up this problem: "cyber workforce management efforts resemble a Ferris wheel: the wheel turns on and on . . . we move, but around and around, never forward."[4]

This paper addresses methods to close the gaps between demand and the current existing capabilities and capacity in the U.S. cyber workforce. A large number of professionals—with not only technical skills, but also an understanding of cyber policy, law, and other disciplines—will be needed to ensure the continued success of the U.S. economy, government, and society in the 21st-century information age. Innovative methods have been developed by the government, think tanks, and private sector for closing these gaps, but more needs to be done. This paper is part of a larger discussion about the future of the U.S. cyber workforce and existing and new concepts that must be expanded to ensure continued success.

The cyber revolution, part of the broader information revolution first defined in 1984, now touches virtually everyone and most aspects of life—80 percent of

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Preparing the Pipeline: The U.S. Cyber Workforce for the Future	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 5th Avenue Ft. Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**16**	

American adults, for example, now use the Internet, as well as over 2 billion people worldwide.[5] The future of the U.S. cyber workforce must consider this great paradigm shift. Increasingly, we encounter "cyber" in our everyday lives: newspapers are online, automobiles contain computerized systems, critical infrastructures such as water, electricity, and communications are networked. Nearly every facet of life has been digitized. Cyber applications impact Federal, state, local, and tribal governments, and businesses depend on cyber-literate employees. Therefore, this paper addresses the need to increase and improve cyber education in the United States while also assessing the centrality of cyber literacy to all levels of education and American society.

according to Congressman Jim Langevin, "growth in demand continues to far outnumber the personnel capable of protecting our networks"

Solutions to the cyber workforce problem are outlined below. The first section of this paper discusses the scope of the problem. The next section covers the paradigm shift in some detail: how existing educational and training pipelines, as well as new ways of thinking and recruiting, are needed. The third section discusses issues particular to state, local, and tribal governments. The final section deals with cyber education at the secondary and postsecondary levels. Finally, a series of initial recommendations are presented.

Scope of the Problem: Existing Pipelines

Within government, industry, and academia, it is universally acknowledged that the cyber workforce needs to be expanded. The 2009 White House Cyberspace Policy Review emphasized both expanding and training the workforce and improving cyber education in order to build greater domestic capacity in the digital age. The Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency lists building an expanded workforce as one of its 10 key recommendations and released a November 2010 report entitled *A Human Capital Crisis in Cybersecurity*. U.S. Strategic Command has identified the Department of Defense (DOD) cyber workforce as undersized and unprepared to meet current and future expected threats.[6] According to Congressman Jim Langevin (D-RI), co-chair of the Congressional Cybersecurity Caucus, the "growth in demand continues to far outnumber the personnel capable of protecting our networks."[7]

The University System of Maryland (USM) Cyber Security Task Force lists "expanding the pipeline for cyber careers" as an actionable recommendation in its 2011 report.[8] Clearly, awareness exists that the current cyber workforce is inadequate.

Before discussing the growth of the cyber workforce, we must develop and agree upon a clearer definition as to who is a member of the cyber workforce. Currently, no specific occupational series identifies Federal cybersecurity positions. In fact, the Government Accountability Office (GAO) lists 17 different occupational series commonly used to label such workers, and this does not even include the uniformed military.[9] As a result, Federal agencies often release highly conflicting information when asked about the size of their cybersecurity workforce: DOD reported 66,000 cybersecurity full-time equivalents (FTEs) in the Office of Management and Budget fiscal year 2010 Federal Information Security Management Act (FISMA) report; 87,846 FTEs in a 2010 agency FISMA report; 88,159 in a 2011 GAO data call; and 18,955 in a 2010 Office of Personnel Management (OPM) study.[10] DOD, Department of Homeland Security (DHS), and other Federal agencies have taken steps to define the roles and responsibilities of the government's cyber workforce, but there is no current and universally agreed upon framework.

Even as the current cyber workforce must grow quantitatively and qualitatively, the gap between

requirements and capacity will no doubt continue to increase exponentially. Within DOD, nearly every combat, logistical, and administrative capability is now digitized and relies on global networks, millions of lines of computer code, and a staff of highly trained information technology (IT) professionals to keep them running and secure. Unmanned aerial systems (UAS) are emblematic of this trend. A UAS is essentially a flying platform composed of varying computerized capabilities, controlled remotely via computer, and usually communicates with a wide range of networked intelligence systems throughout the globe.

As the government's cyber workforce requirements grow, it must also compete with the private sector, both at home and abroad, where demand and incentives (salary, benefits) for talented individuals are highly competitive. Recent years have seen high-profile network intrusions across different commercial sectors, including defense (Lockheed Martin), social media and email (Facebook and Google), finance (Royal Bank of Scotland), IT security (RSA) and entertainment (Sony). To protect and expand their online presence and automated operations, firms not traditionally associated with IT are investing significant resources in their own cyber workforces, further dampening the global competition for cybersecurity professionals. Smaller firms, nonprofits, and any organization with an online presence are forced to make significant cybersecurity investments due to cyber criminals on the lookout for easy prey.

In the near term, attracting talented individuals to expand the cyber workforce will need to be done in an environment of budget austerity. Regardless of the end result of the Federal budget debate, spending will likely be cut across most, if not all, agencies. State and local governments and industry are also facing similar difficulties due to the negative fiscal climate and slow economy. In Congress and on the election trail, there are also influential voices that advocate pushing more responsibilities (and the responsibility for their funding) back on state and local jurisdictions. This should further drive awareness that the push for a more robust cyber workforce will take place in an environment of limited resources, stiff competition, and growing demands.

While there is a debate on how much the overall U.S. cyber workforce must grow, there is wide agreement that—in the face of this growing demand and upcoming retirements—it must grow in both quantity and quality. Due to ageing trends, growth of the overall U.S. workforce is expected to decline from 1.2 percent to 0.8 percent from 2006–2016, and the fastest-growing segment of the workforce is age 55 and older, a segment of the population that tends to be less proficient with technology. In addition, 4-year degrees conferred in computer and information sciences peaked in 2004, and have dropped 30 percent since then.[11] However, other computer-related disciplines and educational/certificate programs have been reported to be on the rise, such as those associated with the computer gaming industry and others that require a great deal of familiarity with computer skills. This makes it difficult to judge the true size of the potential pool of people from which to recruit cybersecurity professionals.

U.S. cyber capabilities and competitiveness strongly underpin the Nation's economic vitality and technological advantage, which in turn underwrite national security and enable the American high standard of living. The United States has been at the forefront of past technological revolutions—industrial, nuclear, space—and a failure to stay at the forefront of the cyber (or information) age could be a serious threat to the American way of life. Despite the growing dependence on cyber and related capabilities, the U.S. scientific and technological base is struggling, and without serious action, there are concerns that it might not be able to sustain a competitive advantage.

Paradigm Shift: Existing Pipelines and New Ways of Hiring

It is clear to cyber experts and observers inside and outside government that many of the terms of the discussion, assumptions, and conventional wisdom need to be updated or discarded altogether. This paradigm shift requires acknowledgment that cyber is now central to

our way of life. Similar to the advent of automobiles and personal computers, the current cyber (or information) revolution puts a versatile device in our hands, pockets, and on our person 24/7. Smart-phones and other advanced computing devices increase productivity in our personal lives, in commerce, and in terms of national security, but these powerful devices also come with significant vulnerabilities. To enable Americans to succeed in cyberspace while simultaneously protecting them in cyberspace, Americans will have to be educated and trained to use these devices effectively and safely at a younger age, even if they are not going into a cyber field of study or occupation. Americans will encounter cyberspace throughout their everyday lives. Similar to learning to drive and learning to read and write, understanding how to operate safely in cyberspace must be recognized as a new core skill for living in the 21st century.

applicants should demonstrate competency prior to being hired, and this competency should not be assumed solely on degrees previously awarded

The concept of what constitutes cyber must also be enlarged from a purely technological notion. There is more to cyber than hardware and software. Computers were created by humans to be used as tools by humans and are fixed, developed, protected and maintained by humans. Investing in people is on a par with, if not more important than, the hardware and software involved. Similarly, while science, technology, engineering, and mathematics (STEM) are the foundation of cyber and other technologies, they are not the only pertinent fields. Although computers date back to World War II, it was innovations in the design and conceptualization of computer technology and an entrepreneurial spirit that brought personal computers into the mainstream and many households. In today's environment, cyber capabilities require legal and policy expertise in order to sift through the development of international norms, rules of engagement, and conflicting statutory authorities, as well as analytical capabilities to identify adversary threats and patterns of behavior. So while the foundation of cyber is STEM, a better understanding and effective use of computers require a truly multidisciplinary approach and a strong investment in human capital.

This paradigm shift also requires a new way of thinking about hiring and recruiting intellectual capital. Currently, the basis for hiring in most government and many private sector positions is the applicant's level of education. Many jobs have minimum educational requirements, and a new employee's salary and level of entry are determined by several factors, education chief among them. While a bachelor's degree is generally required for IT positions, a snapshot of these positions' job descriptions and duties and responsibilities reveals that a 4-year degree (and the types of knowledge, skills, and abilities [KSA] entailed) may be useful for a position, but should certainly not be a prerequisite. In fact, those KSAs can be equally obtained through a combination of technical schools, community colleges, and on-the-job training and experience.

Applicants should demonstrate competency prior to being hired, and this competency should not be assumed solely on degrees previously awarded. Job descriptions and position requirements must be updated to reflect more accurately those KSAs required to perform the job and not only academic credentials or the traditional requirements. This simple change could greatly enlarge the pool of qualified applicants for cyber-related positions.

While competency tests may require more time and cost than an average interview, the institution of such tests would confer several benefits. Government IT departments would instantly know the ability levels of new staff and could adjust training accordingly—and could fast-track the most promising candidates to take advantage of their capabilities immediately. Potential applicants could hone their skills, knowing roughly

what the test requires of them. The difficulty of entrance tests could also be modified based on workforce requirements and the shape of the job market. This market-driven process could work similarly to the military recruiting model.

The most prominent pipelines in place to produce information assurance (IA) professionals for the Federal Government workforce are the National Science Foundation's Scholarship for Service (SFS) and DOD Information Assurance Scholarship Program (IASP). The SFS recruits U.S. citizens in IA education tracks at the undergraduate and graduate levels with scholarships, which are repaid through service to the Federal Government. The IASP has two tracks: a recruitment program to bring new talent into DOD, and a retention program aimed at existing DOD employees seeking to bolster their academic credentials. As scholarship programs, they represent a small percentage of Federal agency IA requirements. From 2001 to 2008, 1,001 students received IA scholarships through these programs, and 93 percent subsequently found employment with the Federal Government. From 2011 to 2013, the Federal Government is expected to hire roughly 8,000 new IA professionals.[12] Clearly, these programs will only address a small fraction of the government's IA workforce requirements and not solve the personnel demands at state and local levels, as well as industry.

Scholarships are expensive solutions, however, and other pipelines are in the process of being built. In 2011, the Defense Advanced Research Projects Agency (DARPA) began Cyber Fast Track, a project designed to award small, short-term contracts to boutique firms and individuals with cyber skills sets needed for the DARPA mission. In the project's research announcement, it notes the strategic mission and seeks solutions to long-term strategic problems such as reducing attack surfaces and vulnerabilities in cyberspace to create greater cost to the adversary.[13] As of December 2011, 13 contracts have been awarded, some of which were of a duration of only 14 weeks and some to firms with as few as five people.[14] Cyber Fast Track has so far successfully bridged the gap between the hacker community and the Federal Government. Similar small and agile concepts, with the potential for bigger payoffs and without the financial or time outlays required by scholarship programs, are solutions that Federal agencies might consider.

A change in our thinking from the cyber domain as purely technological to a domain with a significant human aspect entails the recognition that one of the critical elements of cybersecurity is people—not only a cadre of well-trained individuals ready to respond to security breaches, but also end-users aware of the risks and responsibilities of using government networks. The fact that individuals are generally considered the greatest cybersecurity vulnerability is another reason why investing in people is just as important as investing in hardware and software and may yield a higher return on investment.

Need for a Common Framework and Lexicon across Federal Agencies

Since cybersecurity is a relatively new field, there is no common lexicon or framework for understanding and defining cyber workforce job descriptions. A common lexicon is necessary to assess the true state of the cyber workforce and to model its proper growth. When positions and career paths linking these together are better codified, not only will it become easier to retain talent, but the scope of the workforce problem will become clearer as well.

Such a framework was proposed by the National Initiative for Cybersecurity Education (NICE) in 2011.[15] The stated aim of the NICE Cybersecurity Workforce Framework is to "put forth a working taxonomy and common lexicon that can be overlaid onto any organization's existing occupational structure." The NICE framework organizes positions within the cyber workforce into seven high-level categories under which it groups workers who share major job functions (testing and evaluation, systems administration, and so forth) and finally

Table 1. NICE Cybersecurity Workforce Framework

High-level Categories	Sample Positions
Securely provision: Designing and building secure IT systems	Software engineer, risk/vulnerability analyst, application security tester
Operate and maintain: Providing support, administration, and maintenance	LAN administrator, technical support specialist, database developer, IA security officer
Protect and defend: Identifying, analyzing, and mitigating threats	Blue Team technician, security analyst, network technician, reverse engineer
Investigate: Investigating cyber events or crimes involving IT	Computer network defense forensic analyst, computer crime investigator
Operate and collect: Collecting information used to develop intelligence	Military and intelligence operations
Analyze: Evaluating cyber information to determine intelligence usefulness	Cyber threat analyst
Support: Education and training, policy, legal support for cyber	Legal advisor, information security trainer, information security policy manager

lists sample positions beneath each. The major categories and sample positions are shown in table 1.

Some overlap does exist between certain categories. Immediate incident response, for example, falls under both protect and defend as well as the investigate categories, and network system design, construction, and maintenance all require systems security analysts since networks must be tested both upon launch and continuously throughout their lifespans to ensure viability. NICE recognizes that the existing framework is a work in progress and seeks to refine it through input from academia, business, and nonprofit organizations. Cyber is a growing field and new positions and fields can be added to the framework as technological change alters the landscape of various cyber disciplines. NICE encourages feedback regarding the usefulness of the framework and any inadequacies or suggested improvements.

Cybersecurity at the State, Local, and Tribal Levels

There are several important reasons why state and local jurisdictions are on the frontlines of cybersecurity. For one, state and local governments closely interact with their residents and industry in many ways the Federal Government does not. They maintain many databases containing personally identifiable information (PII), operate e-governance initiatives, and work closely with industry, including companies responsible for critical infrastructure—all of which affect the day-to-day lives of their residents. Due to budget constraints, cybersecurity competes for funding with other state and local priorities, thereby exposing critical infrastructure, residents' PII, and other essential services to vulnerabilities. State and local employees who maintain and protect these information systems are an important, though generally overlooked part of the national cyber workforce. Thus, state and local cyber workforces must not be ignored because of their considerable cybersecurity responsibilities and potential vulnerabilities, and because they are "first responder" assets that can be leveraged in a time of crisis.

What are the potential financial costs of inaction? The 2006 theft of hardware from the home of a Department of Veterans Affairs (VA) employee exposed the PII of 26.5 million veterans and approximately 2

million Active-duty and Reserve military personnel. As a result, VA spent $7 million to notify affected personnel of the data breach, $100 million to offer 1 year of free credit reporting to affected individuals, and also faced a class-action lawsuit from five veterans' groups.[16] The data breach occurred despite repeated warnings from both the GAO and the VA's Inspector General that VA information security management procedures were inadequate.

While the VA example deals with a Federal agency, states have also been in the news for inadequate IT security. An audit conducted by Colorado's Office of Cyber-Security found that PII was easily compromised during a red team penetration test. Colorado estimates a $39.5 million budget shortfall for adequate protection of the state's information systems.[17] The Office of the State Comptroller of New Jersey found that state agencies had failed to remove PII prior to placing surplus equipment up for auction.[18] In 2010, the National Association of State Chief Information Security Officers noted that 79 percent of states saw IT budgets cut or remaining stagnant in the face of rising threats.[19]

One of the primary challenges facing state and local governments is their inability to attract and retain competent individuals. All states, except Vermont, have a legal requirement to balance their budgets. States were hit particularly hard by the 2008 financial crisis, and Federal funding to assist states with budget shortfalls, enacted as part of the 2009 Recovery Act, has expired. Although state finances are improving as the economy begins to recover, states will continue to face historically large shortfalls in the coming years.[20] As a result, states that were once able to attract cyber talent with generous benefits packages are no longer able because of fiscal realities. Impending across-the-board budget cuts will affect not only recruitment, but also the retention of skilled employees. Recent trends indicate that states currently only spend about 2 percent of their IT budget on security, even though the accepted industry standard is about 5 percent.

Some states are also geographically disadvantaged. Top-level talent often receives offers from the private sector and a wide array of Federal agencies. Individuals with low-density, high-demand skill sets generally choose to pursue top-dollar employment options in Silicon Valley and large metropolitan areas rather than geographically remote areas. As stated, state, local, and tribal governments have difficulty competing with salaries and benefits packages offered by the private sector and Federal Government, especially in the current fiscal climate.

states that were once able to attract cyber talent with generous benefits packages are no longer able because of fiscal realities

State and local agencies face tough choices. Some answers to these choices already exist in the form of Federal measures, such as the National Institute of Standards and Technology SP 800-55 and the DHS Risk Management Process. Despite budgetary challenges, state and local authorities may be best served by following Federal Government initiatives and industry best practices by viewing security holistically and not only as an issue of the security of in-house networks. Contractors and third parties that service and connect to government networks must also be part of any solution. What is needed is a comprehensive framework that can be modified depending on the budgetary outlook for a given fiscal year and the current threat environment. Any new framework must not simply be a "check-the-box" bureaucratic exercise, but must be agile and fully evaluate the risks.[21]

Stronger Cyber Education: Not Only a "Pipeline" But Also an "Ecosystem"

Any discussion of cyber education needs to take place at two levels. The first deals with the "pipeline"—that is, the direct channels that will ensure a

trained workforce for U.S. society in the future. The second deals with the "ecosystem"—that is, general cyber education at all levels of schooling that will result in a productive, high-tech workforce for an increasingly cyber-dependent United States. It was this second level the Comprehensive National Cybersecurity Initiative addressed when it stated that "It will take a national strategy, similar to the effort to upgrade math and science education in the 1950s, to meet this challenge."

many high school students seeking to enter STEM fields are unprepared for the scientific and highly technical course material they encounter as freshmen

The demand for professionals with cyber competencies has begun to be addressed by universities. The National Security Agency (NSA) and DHS jointly sponsor the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE), CAE-Research, and community college programs. As of April 2012, these designations have been applied to 145 colleges and universities in the 50 states and Puerto Rico.[22] One outcome of this designation has been a proliferation in quality accredited IA and cybersecurity bachelor's and master's programs nationwide. Students who attend CAE-designated programs are eligible for scholarships and grants through DOD and DHS and upon graduation are immediately ready to enter the workforce for large employers such as the NSA.

The CAE program is expanding in 2012 with a new designation. The CAE–Cyber Operations program is intended to be technical and interdisciplinary, firmly grounded in computer engineering, sciences, and electrical engineering, with extensive hands-on application in laboratories. Expansion likely indicates that the NSA and DHS consider the initial CAE program to be a significant success.

However, distribution of these programs is uneven: of the 145 higher education institutions receiving CAE designation, only 13 are community colleges with "CAE 2-year" designations, and 5 of those are located in the state of Maryland alone. Community colleges often act as trade schools, offering associate's degree programs narrowly focused on a trade, such as paralegal or nursing degrees. California, with only seven schools designated as CAE/IAE, has 5 percent of the designated schools, but represents 12 percent of the U.S. population. In fact, the majority of universities considered among the best computer science programs nationwide have not pursued the designation, including the California Institute of Technology, Massachusetts Institute of Technology, University of Texas at Austin, University of Wisconsin at Madison, and Cornell University to name a few. Why are some of the best STEM schools in the country not applying for CAE designation? More comprehensive study may be required to determine if the degree programs at these universities involve superior models that should be imitated more widely.

Outside of Federal-level initiatives involving higher education, some state education systems have chosen to emphasize cybersecurity at the university level. Previously, Maryland (home to the NSA, U.S. Cyber Command, National Institute for Standards and Technology, Defense Information Systems Agency, and many other Federal agencies and high-tech private-sector firms, such as Lockheed Martin) was mentioned as possessing nearly half of all community colleges in the United States that have received CAE 2-year designations. Maryland also has 13 postsecondary institutions bearing CAE designations, more than any other state. This emphasis has been part of a concerted effort of forward-looking individuals: University System of Maryland Chancellor Dr. William Kirwin convened a task force in November 2010 with representatives from Federal and state government and Maryland universities to examine how the state should approach

cybersecurity. This Cyber Security Task Force is charged with identifying degree requirements for careers in cybersecurity and building USM's related capacity.[23] These initiatives fall under a broader state plan as Maryland has been identified and emphasized as "CyberMaryland" by Governor Martin O'Malley due to its importance for the Federal Government and "hub" status for industry. Since the task force's launch, the number of CAE-designated institutions has grown from 4 to 13. The emphasis placed by state-level offices in Maryland on cybersecurity education could serve as a model for other states.

Broadly speaking, the United States faces a serious challenge in educating the future STEM workforce. A multiyear study conducted by the University of California at Los Angeles concluded that STEM graduates take longer to complete their degrees and are more likely to drop out than those in non-STEM fields.[24] Among the causes are that teaching quality in STEM disciplines often suffers as faculty prioritizes research that contributes to tenure track and grant funding in many institutions. In addition, the lack of mentorship and research opportunities for undergraduates also discourages many. Proper preparation is also cited as a problem: many high school students seeking to enter STEM fields are unprepared for the scientific and highly technical course material they encounter as freshmen. At the high school level, a shortage of qualified teachers means that students are not exposed to programming or computer science, which means that by the time they reach the undergraduate level, many have already chosen a course of study and mapped out their degree path (and cyber is not part of it).

Cyber is a wider discipline than simply the STEM fields, and professionals with backgrounds ranging from the social sciences to business and the arts will be needed in the cyber workforce of the future. Nonetheless, the Federal Government must consider measures to improve STEM education and work to increase the number of future engineers and mathematicians who matriculate since these and other STEM areas are the foundational fields of cyber.

At the high school and college levels, there are two ways to prepare students for future employment as part of the cyber workforce. Students can either focus on cyber-related disciplines as part of their core coursework or focus on cyber-related studies as electives or extracurricular activities. One example of a program that confers college-level classroom experience on high school students is the Alamo Academies in San Antonio. Meanwhile, the U.S. Cyber Challenge competition assesses the cyber aptitude of high school students, college students, and young adults through a series of tournaments. Both programs have resulted in direct employment of graduating seniors in IT positions in government and with defense contractors.

Alamo Academies is unique in its level of partnership with industry, local government, public school systems, and community colleges

As a successful example of "preparing the pipeline," it is important to examine the role of industry in driving the initial creation of the Alamo Academies. Following the closure of Kelly Air Force Base in 1997, Lockheed Martin and Boeing accepted a large logistics contract and hired a third of the former installation's workforce to execute it. Aware that a large segment of their workforce would begin retiring in the next 10 years, these companies began consulting with nearby San Antonio Community College about how well its curriculum matched their entry-level workforce requirements. Stemming from those discussions, and initial successes, a program was instituted with the Aerospace Academy in 2001. Today, 220 high school juniors and 168 high school seniors are enrolled in the Alamo Academies program.

The Alamo Academies consists of programs at five San Antonio and Bexar County schools: San Antonio, St. Philip's, Palo Alto, Northeast Lakeview, and Northwest Vista. All five offer associate's degree programs and certificates and licensure in occupational programs that prepare students for jobs in the local and regional

Table 2. Selected U.S. Cyber Competitions

Competition	Audience	What It Does	Web Links
Cyber Security Treasure Hunt	High school students, college students, and adults who want to prove they have basic mastery of IT security	Like a scavenger hunt, the game delivers an online quiz that sends candidates to a simulated environment where they can safely explore and find answers to questions.	http://securitytreasurehunt.com/
Cyber Foundations High School Competition	High school students	Students receive basic instruction in three modules: networking, operating systems, and system administration, and then are quizzed on knowledge of the systems.	https://www.cyberfoundations.org/
Cyber Patriot High School Defense Competition	High school students	Students must harden systems to block attacks and are scored on their success in keeping the attackers out.	www.uscyberpatriot.org/Pages/default.aspx
U.S. Cyber Challenge Summer Camps	College students and some high school students, depending on location	Week-long "boot camps" focusing on intensive instruction on penetration testing, reverse engineering, and forensics, all culminating in competitions.	https://www.nbise.org/uscc/camps/
DC3 Digital Forensics Challenge	Separate challenges for high school students, college students, and adults to demonstrate forensics skills	Provides a disk image of data taken from actual cases investigated and asks four levels of questions; the fourth level includes questions even DC3 has been unable to answer.	www.dc3.mil/challenge/2011/

Table 2. cont.

National Collegiate Cyber Defense Competition	College students	Students compete in a simulation where they manage a small business IT system and protect against attacks.	www.nationalccdc.org/
SANS NetWars	Talented high school students, college students, and adults	Students work in a real-world, online laboratory attempting to capture and hold territory in cyberspace while hundreds of others attempt to do the same.	www.sans.org/cyber-ranges/netwars/

economy. All courses are fully transferable to colleges and universities across the United States. The objective of the Alamo Academies is to accelerate the learning of future cyber workforce members. The program allows high school juniors and seniors to complete college-credit coursework on local campuses where they take approximately half of their classes at their high school and the remainder at the community college. Students study in one of four degree programs: aerospace academy, IT security academy, manufacturing academy, or the health professional academy.

While other programs similar to the Alamo Academies exist around the United States, few exist at the high school level, and it is unique in its level of partnership with industry, local government, public school systems, and community colleges. High school juniors and seniors must pass college assessment tests in order to enter the program. Students have the flexibility to study at the Alamo Academies in the morning or evening depending on their schedules. These students are also given a chance to practice what they learn on the job via paid summer internships with locally based defense contractors and other major corporations, including Lockheed Martin, Boeing, Toyota, ITM, Kinetic Concepts, Cox Manufacturing, AT&T, and SWBC. Class sizes are limited because technical courses cannot have more than a 12-to-1 student/teacher ratio, and the program size is determined by the number of internships offered by local businesses in a given year.

Equally important are the financial details of the program. Students' tuition and fees are waived and transportation to the Alamo Academies and textbooks are provided by local school districts. Bus fleets are reimbursed by the state of Texas through support to technology initiatives, and community colleges receive funding via taxes and state education funds that allow them to waive tuition and fees for high school students. School districts receive funding based on how many students attend each school, and as the Alamo Academies's students spend half of their day at their home high schools, the school districts' funding is unaffected.

The U.S. Cyber Challenge is composed of several components targeting students of various skill levels and in different venues. The lowest rung operated by U.S. Cyber Challenge is Security Treasure Hunt, an online environment that assesses student skills in different information security areas, including Web vulnerability assessment, digital forensics, cryptographic analysis, and

penetration testing.[25] U.S. Cyber Challenge is open to the public with the stated objective of identifying individuals with promising skills in information assurance.

Part of the Treasure Hunt, Cyber Quests, attracted 800 participants from 400 different schools. The 200 winners (all high school and postsecondary students) were offered slots in weeklong summer cyber camps, held at various colleges and universities around the United States. The camps are designed as "cyber boot camps" where attendees gain in-depth knowledge of penetration testing, forensics, and reverse engineering from university-level faculty. Winners of the end-of-camp "capture the flag" tournament were offered $1,000 scholarships by (ISC)², a well-known educator and industry credentialing authority.[26]

both the pipeline and ecosystem need to be improved to increase the size of the cyber workforce and better prepare the United States for future security challenges

Another program, Cyber Patriot, began in 2008 as a national high school cyber defense competition organized by the Air Force Association (AFA). Initial competitions were held in 2009 with over 200 teams participating. Similar to the formation of the Alamo Academies, a partnership between industry and academic institutions played a prominent role in the launch of Cyber Patriot. Along with AFA, defense contractor SAIC and the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio worked together to stand up Cyber Patriot. In addition, Northrop Grumman committed the funding for Cyber Patriot to operate nationwide. The 2011 competition features 2,500 teams from all U.S. states.

The National Collegiate Cyber Defense Competition (NCCDC) is another university-level event that provides more of a "regular season" for college teams rather than limited "tournament" play. First launched in 2005 by CIAS—also a Cyber Patriot sponsor—the NCCDC that began in April 2011 featured 9 regional finalists from more than 100 teams nationwide. The NCCDC also includes participation from the private sector, including Deloitte LLP (the 2011 title sponsor), as well as Microsoft, McAfee, SAIC, Boeing, Northrop Grumman, Red Lambda, and Zynga.[27]

The DOD Cyber Crime Center Digital Forensics Challenge dates back to 2006. It is an individual competition where competing teams gauge their success based on the number of possible points achieved in each challenge. The focus is on uncovering digital evidence from a network breach. Open to international competitors, the 2010 Grand Champion was a team from South Korea. Prizes are also awarded to the best teams from several different categories, including U.S. Government, military, civilian, graduate, undergraduate, community college, and high school.[28]

NetWars is sponsored by the SANS Institute, an industry-credentialing authority and educator, and is aimed at all skill levels. During this competition, all players begin on the same footing, but only professionals with at least 10 years of experience are expected to perform at the top level. SANS also conducts NetWars Continuous, which is a similar challenge, but during a 4-month league rather than tournament format.[29]

Whom should these competitions target? According to the director of the U.S. Cyber Challenge, these competitions should aim to attract students in non-STEM fields. Many of these students have skills, but due to misconceptions about "technology," they are reluctant to participate. Nevertheless, after joining, many of these students have found success in Cyber Challenge and other competitions. In fact, marketing, communications, arts, and business majors, all of whom are disproportionately underrepresented in cyber and STEM fields, have done quite well in various cyber competitions over the years.

Concluding Thoughts

Both the pipeline and ecosystem need to be improved to increase the size of the cyber workforce and better prepare the United States for future security challenges. Should current trends hold in the future, cyber will be even more interwoven into the fabric of every-

day life in the United States. Outside of STEM, a more thorough dialogue is necessary about cyber education at the secondary level. Not only should this education be about how to use computers, but how to navigate and operate safely in cyberspace in order to best take advantage of it. The concept of the "cyber playground" has been raised as an analogy. How do you teach children to play safely on the playground in the absence of adults? Understanding the dangers inherent in Internet use is not widely held, and education at lower levels is rudimentary, merely focusing on using computers. Eventually, greater understanding of cyberspace and its dangers will need to be integrated into curricula at the secondary level. And at home, if awareness of these technologies and their dangers is not present in the minds of the young, network security as a whole is likely to continue to suffer in the future because of poor end-user practices and habits.

Integrating cyber education at a low level into primary and secondary school curricula may have added benefits as well. The introduction of computers and the Internet at a young age may lead to more individuals pursuing cyber and STEM-related coursework in elementary through high school. This would likely increase the size and interest of cyber and STEM students in postsecondary educational institutions, thus ensuring a strong ecosystem to supply the pipeline into the U.S. cyber workforce.

Recommendations

Federal Government hiring rules and authorities for cyber workforce professionals: There exists a need to explore alternative hiring authorities for cyber professionals, including education-based, skills-based, and experience-based processes. Recommend forming a DHS/DOD/OPM task force to examine core workforce issues and provide short-, mid-, and long-term human capital strategies for government departments and agencies.

Federal Government career path and progressions for cyber workforce professionals: There is presently no formal career path for government employees in the field of cybersecurity. A large percentage of cybersecurity has been outsourced to the private sector. Recommend OPM consider creating a government career series, classification standards, and promotion path for a new cybersecurity career series.

integrating cyber education at a low level into primary and secondary school curricula may have added benefits

A career path should also be formalized for our cyber senior leaders, which would focus on not only technical competence, but also organizational management and decisionmaking regarding complex cyber issues. This senior leader career path should also require cross-organizational or "joint" training and development as cyber decisionmakers would greatly benefit from experiences in DOD, DHS, the private sector, and other cyber-related organizations.

State and local government issues for cyber workforce professionals: State, local, and tribal governments are facing enormous fiscal pressures and have not invested or cut back their investment in cybersecurity related activities. This has disincentivized the local workforce from pursuing this career field. Recommend the Congress consider legislative incentives (matching funds) for investment in cybersecurity. Also, recommend the Federal Government seek standardization of cybersecurity workforce positions with state, local, and tribal governments and explore methods for easier transfer of cybersecurity professionals among the different levels of government and with select private sector partners.

Streamlined security clearance process: Many cybersecurity positions require some form of security clearance. The current vetting for security clearances is cumbersome and time consuming and potentially disincentivizes many to apply for positions requiring a clearance. This applies to potential government employees and civilian partners where classified information-sharing is critical. For example, DOD relies on the

Global Transportation Network both to protect power and for sustainment. Nearly 85 percent of this network is owned by the private sector. The United States must be able to share information with these critical private sector partners to help protect this critical capability. Recommend that specific guidelines and processes be developed for potential employees (both government and private sector) in the cybersecurity workforce. The goal is to accelerate the process and empower select private sector partners with critical information without compromising standards.

Congressional advocacy: As of May 2012, there were several major cybersecurity bills pending in Congress. Each represents a significant step forward in the recognition of the criticality of the cybersecurity issue. It might be useful if Congress would consider designating the cyber workforce issue for the U.S. Government and U.S. society as a whole to specific oversight committee(s) that would be responsible for introducing appropriate legislation and monitoring progress on this issue.

Public-private solutions for enhancing the cyber workforce pipeline: The private sector has recognized the potential shortfalls in the future cyber workforce and has made modest strides toward developing their own future workforce. Recommend OPM and the Department of Education consider building off of these private sector initiatives and develop or facilitate development of similar intern/scholarship programs.

Broader educational initiatives to emphasize and improve STEM education and cyber-related competencies (such as legal, policy, and intelligence analysis): There are a number of well intended but disconnected STEM initiatives under way in the government and private sector. Recommend that the executive branch consider making this a national priority included in a national "Competitiveness Strategy."

National strategic communication campaign to emphasize the importance of cyber and STEM education: STEM education is one of the key building blocks for U.S. competitive advantage in the cyber domain and many other fields. Recommend the executive branch, Department of Education, and Congress consider creating incentives via funding, grants, prioritization, and public recognition for students, educators, public officials, and professionals to place a renewed emphasis on STEM education as a necessity for sustaining U.S. prosperity and global leadership.

Notes

[1] Partnership for Public Service, *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce* (Washington, DC: Booz Allen Hamilton, July 2009), available at <www.ourpublicservice.org/OPS/publications/download.php?id=135>.

[2] Remarks by Secretary of Defense Robert Gates at Maxwell Air Force Base, Alabama, April 15, 2009, available at <www.defense.gov/transcripts/transcript.aspx?transcriptid=4403>.

[3] Office of the Inspector General, *The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat*, Audit Report 11-22 (Washington, DC: Department of Justice, April 2011), available at <www.justice.gov/oig/reports/FBI/a1122r.pdf>.

[4] Jason Healey, "Cyber Workforce Ferris Wheel," *New Atlanticist Policy and Analysis Blog*, May 3, 2011, available at <www.acus.org/new_atlanticist/cyber-workforce-ferris-wheel>.

[5] Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, 2 vols. (Washington, DC: Center for New American Security, June 2011), 11.

[6] Government Accountability Office (GAO), *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, GAO-11-75 (Washington, DC: GAO, July 2011), available at <www.gao.gov/assets/330/321818.pdf>.

[7] James Langevin, "Preparing the Pipeline: U.S. Cyber Workforce for the Future Workshop," Presentation at National Defense University, October 12, 2011.

[8] "Mikulski Joins USM Chancellor Kirwan to Release Cyber Security Task Force Report," Press Release, May 23, 2011, available at <http://mikulski.senate.gov/media/pressrelease/0523112.cfm>.

[9] GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, DC: GAO, November 2011), available at <www.gao.gov/new.items/d128.pdf>.

[10] Ibid.

[11] *Netgeneration: Preparing for Change in the Federal Information Technology Workforce* (Washington, DC: Chief Information Officers Council, April 2010), available at <www.cio.gov/Documents/NetGen.pdf>.

[12] Juan Lopez, Jr., and Richard A. Raines, "Maximizing the DoD Return on Investment in Cyberspace Professionals," *IATAC IA Newsletter* 13, no. 3 (Summer 2010), 18.

[13] Dawn Lim, "DARPA's New 'Fast Track' Okays Hacker Projects in Just Seven Days," *Wired,* November 14, 2011, available at <www.wired.com/dangerroom/2011/11/darpa-fast-track/>.

[14] Austin Wright, "With Cyber Fast Track, Pentagon funds hacker research," *Politico*, December 7, 2011, available at <www.politico.com/news/stories/1211/70016.html#ixzz1fwc5qStN>.

[15] "NICE Cybersecurity Workforce Framework," National Institute of Standards and Technology, September 2011, available at <http://csrc.nist.gov/nice/framework/>.

[16] Sidath Viranga Panangala and Alison M. Smith, *Theft of Veterans' Personal Information, and Department of Veterans Affairs Information Technology Reorganization: Issues for Congress*, RS22460 (Washington, DC: Congressional Research Service, June 22, 2006).

[17] Tim Hoover, "Colorado's state computer systems fail 'hacker' test in cyber-security audit," *The Denver Post*, December 14, 2010, available at <www.denverpost.com/legislature/ci_16852217>.

[18] Office of the State Comptroller, State of New Jersey, "Comptroller audit finds state agencies failed to remove confidential information from computers packaged for public auction," March 9, 2011, available at <www.nj.gov/comptroller/news/docs/press_surplus_audit_03_09_2011.pdf>.

[19] "State governments at risk: A call to secure citizen data and inspire public trust," 2010 Deloitte–National Association of State Chief Information Security Officers Cybersecurity Study, available at <www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.PDF>.

[20] Phil Oliff, Chris Mai, and Vincent Palacios, "States Continue to Feel Recession's Impact," Center on Budget and Policy Priorities, June 27, 2011, available at <www.cbpp.org/cms/?fa=view&id=711>.

[21] "State governments at risk."

[22] National Security Agency, Centers of Academic Excellence, available at <www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml>.

[23] University System of Maryland (USM), *Report on the Cyber Security Task Force to the University System of Maryland, May 2011* (College Park, MD: USM, June 2011), available at <http://mdcao.usmd.edu/USMCyberSecurity_final.pdf>.

[24] Higher Education Research Institute, "Degrees of Success: Bachelor's Degree completion rates among Initial STEM majors," Research Brief, January 2011, available at <www.heri.ucla.edu/nih/downloads/2010%20-%20Hurtado,%20Eagan,%20Chang%20-%20Degrees%20of%20Success.pdf>.

[25] U.S. Cyber Challenge Security Treasure Hunt, available at <http://questionengine.securitytreasurehunt.com>.

[26] "U.S. Cyber Challenge announced 2011 Cyber Camps," *PRWeb*, June 22, 2011, available at <www.prweb.com/releases/2011/6/prweb8583320.htm>.

[27] Christi Fish, "College students gather for cyber defense competition nationals April 8-10," *UTSA Today* (San Antonio), April 7, 2011, available at <http://utsa.edu/today/2011/04/cybersecfinals.html>.

[28] "2010 DC3 Challenge Stats—Winner's Circle," Digital Forensics Challenge, May 17, 2011, available at <www.dc3.mil/challenge/2010/stats/winners.php>.

[29] SANS NetWars, available at <www.sans.org/cyber-ranges/netwars/>.

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The Center for Technology and National Security Policy (CTNSP) within the Institute for National Strategic Studies helps national security decisionmakers and their staffs understand emerging impacts of technology and integrate them effectively into policies through research, teaching, and outreach. CTNSP supports the Department of Defense leadership and Congress while also encouraging whole-of-government and public-private collaboration.

The Defense Horizons series presents original research by members of NDU as well as other scholars and specialists in national security affairs from the United States and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Defense Department or any other agency of the Federal Government. Visit NDU Press online at www.ndupress.edu.

Linton Wells II
Director
CTNSP

COL Timothy A. Vuono, USA
Director, INSS
Director of Research

Francis G. Hoffman
Director
NDU Press

Other titles from NDU Press

For online access to NDU Press publications, go to: ndupress.ndu.edu

Offshore Control: A Proposed Strategy for an Unlikely Conflict
by T.X. Hammes
(Center for Strategic Research, Strategic Forum 278, June 2012)

Grand Strategy and International Law
Nicholas Rostow
(Center for Strategic Research, Strategic Forum 277, April 2012)

Cross-currents in French Defense and U.S. Interests
Leo G. Michel
(Center for Strategic Research, Strategic Perspectives No. 10, April 2012)

Russia and the Iranian Nuclear Program: Replay or Breakthrough?
John W. Parker
(Center for Strategic Research, Strategic Perspectives No. 9, March 2012)

Post-Asad Syria—Opportunity or Quagmire?
Patrick Clawson
(Center for Strategic Research, Strategic Forum 276, February 2012)

Space and the Joint Fight
Robert L. Butterworth
(Center for Strategic Research, Strategic Forum 275, February 2012)

Raising Our Sights: Russian-American Strategic Restraint in an Age of Vulnerability
David C. Gompert and Michael Kofman
(Center for Strategic Research, Strategic Forum 274, January 2012)

Sino-American Strategic Restraint in an Age of Vulnerability
David C. Gompert and Phillip C. Saunders
(Center for the Study of Chinese Military Affairs, Strategic Forum 273, January 2012)

Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?
Vincent Manzo
(Center for Strategic Research, Strategic Forum 272, December 2011)

The Emergence of China in the Middle East
James Chen
(Center for the Study of Chinese Military Affairs, Strategic Forum 271, December 2011)

A Review of the 2001 Bonn Conference and Application to the Road Ahead in Afghanistan
Mark Fields and Ramsha Ahmed
(Center for Strategic Research, Strategic Perspectives No. 8, November 2011)